Висновок

В роботі знято обмеження щодо використання сигналів частоти полів в системах цифрового телебачення стандартної чіткості, введені Рекомендацією ITU-R BT.801-1, та запропоновано використання цих сигналів в системах високої чіткості з прогресивною, черезрядковою розгорткою та з передачею сегментованих кадрів. Запропоновано відповідні набори параметрів для систем ТБВЧ.

Дана модель є несуперечливою з описом частоти полів, що його реалізовано в існуючому випробувальному телевізійному обладнанні.

Список літератури: 1. Випробувальні сигнали для оцінювання якості роботи відеотрактів систем цифрового ТВ мовлення / О.В. Гофайзен, Мохаммед Хасан Хессейн Алі, В.В. Пилявський // Восточно-Европейский журнал передовых технологій. – 2011. – №4/9(52). – С.51. 2. http://www.testequipmentsolutions.com.au/products/SAF_SFF.pdf. 3. http://www2.tek.com/cmsreplive/psrep/13328/20W_17828_3_2011.01.05.13.16.16_13328_EN.pdf 4. http://www.cnrood.com/PHP/files/instrum_pdf/TG-2000.pdf. 5. http://chesterviewltd.com/pdf/CVBlackV96.pdf.

Поступила в редколлегию 09.09.2011

УДК 621.391

***А.В. ПЕРСИКОВ*, канд. техн. наук,** доц., ХНУРЭ, Харьков
А.С. ЕРЕМЕНКО, с.н.с., ХНУРЭ, Харьков

ПРОТОТИП УЛУЧШЕННОГО ПРОТОКОЛА ОБМЕНА ДАННЫМИ МЕЖДУ СИСТЕМАМИ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ АТАКАМ

В статті аналізуються недоліки сучасних протоколів обміну інформацією між системами виявлення та протидії атакам та пропонується прототип покращеного протоколу, орієнтованого на надійну захищену передачу інформації в потенційно вразливих різнорідних мережах.
Ключові слова: атака, самоопис, алгоритм, метріка

In the article the shortcomings of modern communication protocols between intrusion detection and prevention systems are analyzed. The prototype of the improved protocol which is reliable secure data transmission-oriented in the potentially vulnerable heterogeneous networks is proposed.
Key words: attack, self-description, algorithm, metric

В статье анализируются недостатки современных протоколов обмена информацией между системами обнаружения и противодействия атакам, и предлагается прототип улучшенного протокола, ориентированного на надежную защищенную передачу информации в потенциально уязвимых разнородных сетях.
Ключевые слова: атака, самоописание, алгоритм, метрика

1. Введение

Публичные сети, такие как Интернет и интегрируемые с ним сети, являются общедоступными телекоммуникациями, сервисами которых пользуются миллионы пользователей. Ежедневно в публичных сетях производится несколько сотен тысяч попыток прекращения работы сетей в целом, которые инициируются

в основном профессиональными злоумышленниками, обладающими специальным программным инструментарием и аппаратной базой со значительной вычислительной мощностью [1].

Поэтому актуальной проблемой для такого вида сетей является обеспечение информационной безопасности (ИБ), которое подразумевает реализацию различных процедур и задач: аутентификации, идентификации, авторизации, аудита, конфиденциальности и целостности информации и других [2, 3]. Предотвращение атак только в определенном сегменте крупной или мелкой сети в принципе не имеет смысла, поскольку сети на основе технологии коммутации пакетов и протокола IP являются отказоустойчивыми вследствие возможности выбора множества путей следования информации [4]. Поэтому злоумышленник имеет возможность обходить защищенные сегменты и распространять свои действия на незащищенные [1].

Использование пассивных средств защиты, способных производить аудит событий и фильтрацию данных не дает должного эффекта, поскольку такие средства защиты не способны давать количественную оценку состояния сети [2]. Акцент в современных системах защиты должен делаться на использовании активных средств защиты, способных аккумулировать данные о различных событиях в сети, производить многокритериальный анализ этих данных и воздействовать на состояние сетевых элементов с помощью общих или специальных интерфейсов [2] (т.е. проводить активный аудит).

Основным средством обеспечения масштабируемой активной защиты является внедрение распределенных систем обнаружения и противодействия атакам (intrusion detection and prevention systems, IDPS) [5]. IDPS должна поддерживать работу в режиме реального времени для проведения следующих операций:

−реализации механизмов защиты, соответствующих политике безопасности сети;

−определения вторжения и предсказания намерений и действий злоумышленника;

−оценки потенциальных уязвимостей, сбора данных и анализа текущего состояния сети и системы защиты;

−проведения ответных действий, включая подавление действий злоумышленника и перераспределение нагрузки между критически важными защитными механизмами;

−уменьшения последствий вторжения и определения уязвимостей, адаптации системы ИБ для лучшего противодействия уже изученным атакам в будущем.

Недостатком современных IDPS является отсутствие эффективных протоколов обмена данными, которые позволяли бы обмениваться данными между IDPS различных производителей [5], ориентированных на различные форматы хранения и обмена данными. Протоколы, предлагаемые сообществом Интернет [6, 7] находятся в стадии экспериментального тестирования и не отвечают всем требованиям современных систем защиты [2]. Кроме того, данные протоколы рассматривают лишь задачу универсального форматирования данных,

но не освещают вопросы динамического обнаружения элементов IDPS в сетях и маршрутизации данных в потенциально уязвимой сети.

Поэтому актуальной проблемой и задачей является разработка прототипа универсального протокола (стека протоколов) обнаружения IDPS и обмена данными между IDPS различного типа. Протокол должен быть способен доставлять данные с временными и качественными характеристиками, задаваемыми каждым из видов сетей, учитывающего потенциальную опасность передачи данных посредством определенного канала связи или подсети.

2. Основные требования к современным защищенным протоколам обмена данными в рамках IDPS

На сегодняшний день не существует стандартизированных протоколов универсального обмена информацией между различными IDPS [5]. В качестве предлагаемого протокола в экспериментальной стадии разработки находится протокол IDXP [6], однако данный протокол ориентирован лишь на решение задачи универсального форматирования данных (в рамках IDMEF [7]). Анализ возможностей IDXP/IDMEF показал, что:

1) протокол не решает вопросы фазы переговоров о выбираемых технологиях обмена информацией (включая протоколы и криптографические алгоритмы);

2) протокол является прикладным и ориентированным на соединение типа «точка-точка», что предполагает использование служебного транспортного протокола, который может быть скомпрометирован до организации защищенного канала обмена данными;

3) протокол декларирует возможность многоканального (многопутевого) обмена данными, но не описывает его;

4) отсутствует реализация пула соединений, вследствие чего возникает необходимость повторного формирования защищенного канала при последовательной передаче сообщений.

Однако, не смотря на указанные недостатки, идеи IDXP/IDMEF можно использовать в прототипе протокола для решения задач универсального форматирования данных.

Прототип протокола должен базироваться на сетевом уровне (может быть выбран подход, аналогичный определенному в протоколе IPv6 [8]) для выполнения маршрутизации данных и ускоренного обнаружения устройств за счет посылки сигналов-фреймов о присутствии объекта IDPS определенного типа [9, 10]. Обеспечение взаимной аутентификации сетевых элементов в данном случае может быть реализовано за счет применения протокола EAP [11].

Для доставки сообщений между хостами, где работает IDPS, может быть использована связка «маршрутизируемый протокол – транспортный протокол». В качестве маршрутизируемого протокола могут быть выбраны IPv4 и IPv6 [4] (в случае применения криптографической защиты – IPsec [12]), а в качестве транспортного – BEEP-инкапсулированный [14] протокол TCP [15]. В принципе, рассматривая IDPS как маршрутизирующее устройство, способное контролировать состояние маршрутизаторов в сети, можно создать наложенную

сеть обмена информацией, относящейся к задачам обнаружения и противодействия атакам.

Доставка сообщений, содержащих описание различных видов уязвимостей и способы противодействия им должна осуществляться с использованием универсального формата данных, которым является текстовый формат. Разметка текстовых данных может осуществляться с помощью определенного языка разметки, базирующегося на спецификации SGML [16]. Поскольку предполагается, что прототип протокола совместим с IDXP, то в качестве языка разметки будет выбираться XML. Для кодирования информации может использоваться стандарт MIME [17], а в случае применения криптографической защиты – S/MIME [18]. В случае применения S/MIME реализуется шифрование (опционально – с сжатием) передаваемых сообщений и поэтому сервисы защиты сетевого уровня можно ограничить взаимной аутентификацией узлов и согласованием сеансовых ключей – фактически отпадает необходимость в формировании полноценного криптографического туннеля между хостами, где функционируют IDPS, что увеличивает скорость работы системы в целом [13]. Данный аспект важен при масштабировании объединения систем IDPS и одновременной работе десятков тысяч сенсоров [19]. Управление запросом/отдачей данных может осуществляться на основе протокола HTTP [20], что позволит передавать сигнальную информацию в разнородных сетях, где применяется межсетевое экранирование [2] (поскольку прохождение сообщений протокола HTTP обычно не блокируется).

Второй задачей (после обеспечения совместимости систем путем унификации формата представления данных), решаемой при выборе языка разметки данных, является задача обеспечения не увеличения уровня неопределенности состояния сети по мере получения новых данных в IDPS от других IDPS. Уровень неопределенности увеличивается, в следующих случаях:

1) получении некорректных данных, навязываемых злоумышленником;

2) получении поврежденных данных, которые будут некорректно интерпретироваться;

3) запоздалом получении данных вследствие задержек в сети (в том числе и вызванных воздействием атак), несвоевременности посылок данных, а также необходимости конвертации данных;

4) получении корректных данных, но представленных в другом формате (приводит к увеличению общего числа состояний системы).

Противостоять навязыванию данных злоумышленником возможно за счет использования примитивов обеспечения целостности [13] и специальной разметки MIME (S/MIME). Тэговая разметка протокола XML позволяет обнаруживать несоответствия синтаксиса [21] и, таким образом, выявлять некорректные фрагменты сообщений. Это позволит избежать передачи в систему анализа некорректных данных (в том числе. И представленных в другом формате). Запоздалой доставки данных можно избежать за счет использования ориентации на управления трафиком Traffic Engineering [22] и использования резервирования ресурсов по пути следования данных. В случае если трафик не

доставляется по определенному множеству путей заданное количество раз, эти пути должны быть исключены из топологии сети.

3. Этапы работы протокола обмена данными

Прототип протокола состоит из трех этапов, каждый из которых в свою очередь состоит из определенного числа фаз (рис. 1). Деление на фазы и этапы производится таким образом, что действия в рамках этапа могут выполняться циклически, а переход от одного этапа к следующему возможен лишь в случае успешного завершения всех фаз этапа.

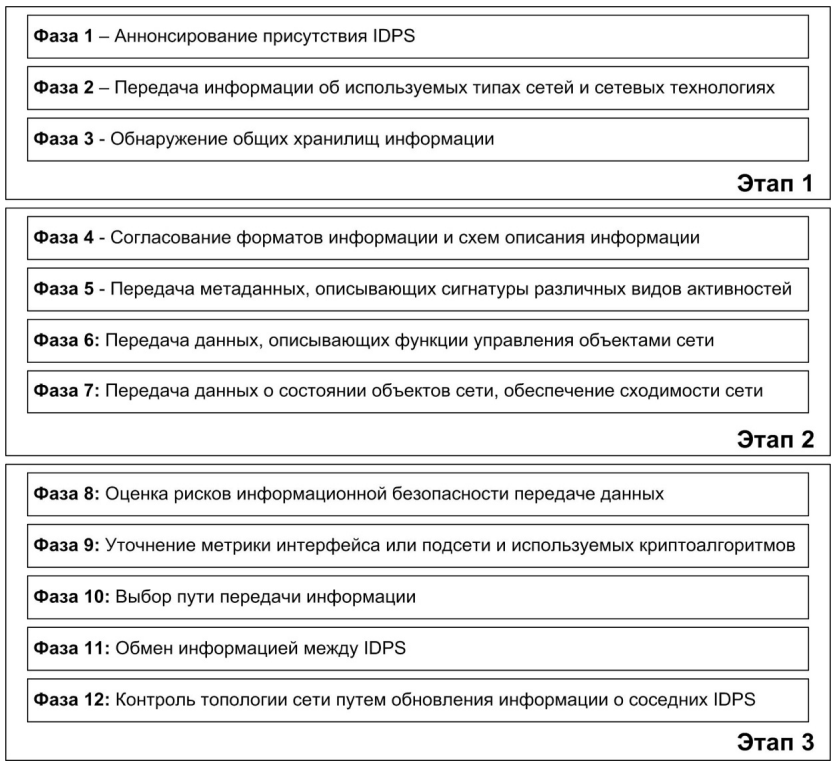

Рис.1. Задачи, выполнение которых поддерживает протокол обмена данными

Большинство из фаз являются самостоятельными элементами протокола и могут исполняться независимо от других фаз. Это дает возможность параллельного выполнения действий в рамках протокола с постоянным изменением представлением сети в рамках объединенной системы IDPS. Передача информации и управление сетью в таком случае можно выполнять итеративным способом, т.е. управление будет улучшаться по мере получения дополнительной информации [23].

Акцент в протоколе обмена информацией в рамках объединенной системы IDPS должен делаться на обеспечении возможности неухудшения представления о состоянии сети и получении только актуальной ненавязываемой злоумышленником информации. Рассмотрим подробно идеи, реализуемые в рамках каждого из этапов.

4. Реализация фаз этапа обнаружения смежных IDPS

Аннонсирование присутствия IDPS (фаза 1) выполняется с использованием широковещательных и многоадресных рассылок на основе стандартных протоколов стеков IPv4 и IPv6 [4, 9]. Обязательным требованием к началу санкционированного обмена данными является проведение аутентификации источника информации (или взаимной аутентификации узлов в случае двуточечного обмена данными). Для реализации аутентификации в сети с гибкой топологией может быть использован подход, рекомендуемый для сенсорных сетей на базе IEEE 802.15.4 [24, 25]. Ограничением подхода, описываемого в [25] является отсутствие масштабируемости сети по причине малого количества ресурсов устройства, однако такое ограничение отсутствует для IDPS.

Передача информации об используемых типах сетей и сетевых технологиях должна выполняться различными способами для обеспечения универсальности механизма обмена информацией в рамках разнотипных сетей. Возможно применение системы DNS [26, 27], сетевого каталога (СК) [28] или базы данных SNMP [29] (табл. 1).

Наиболее масштабируемым решением является использование системы DNS (путем внесения информации в записи типа HINFO [26]) с применением DNSSEC (гарантирует высокий уровень криптографической защиты и позволяет эффективно управлять криптографическими ключами на основе сертификатов) [27]. Данный сервис является уже реализованным для использования в Интернете. Ограничениями DNS являются возможность использования только в сетях TCP/IP и низкая скорость работы в случае применения DNSSEC.

Служба каталога X.500 позволяет группе IDPS взаимодействовать с телекоммуникационными системами (ТКС) различного типа, управлять сертификатами открытого ключа и эффективно структурировать сетевые ресурсы. СК требует значительного количества системных ресурсов для его инсталляции, и его скорость работы является посредственной.

SNMP MIB является наименее ресурсоемким решением, однако масштабируемость базы данных SMNP является очень низкой. Также SNMP не позволяет одновременно использовать множество криптоалгоритмов для преобразования трафика.

Все системы (DNS, X.500 и SNMP) поддерживают анонсирование информационной базы в сети (фаза 3).

5. Реализация фаз этапа согласования параметров объединенной системы IDPS

Согласование форматов информации (фаза 4) предполагает выбор формата обмена информацией и способа преобразования информации (специальное кодирование и/или шифрование). Как было сказано ранее, для обмена сообщениями между разнотипными системами эффективным и хорошо зарекомендовавшим способом является использование протокола MIME и разметки данных на основе XML.

Эффективность XML объясняется тем, что модель данных в случае применения XML является управляемой содержимым данных – новые объекты вводятся с целью добавления новых уведомляющих данных и при этом отсутствуют семантические различия между уведомлениями. Это очень важная цель, поскольку задача классификации и именования уязвимостей ТКС является очень сложной и очень субъективной.

XML допускает слияние схем именования и описания объектов, что важно при согласовании метаданных (фаза 5), применяемых для записи сигнатур. Передача информации в случае представления функциональности IDPS в виде веб-сервисов (современный подход, когда функции защиты реализуются в виде сетевого сервиса) может реализовываться с применением протокола SOAP [23]. Такой же подход используется и для передача данных, описывающих функции управления сетью (фаза 6).

Сходимость сети (фаза 7) должна обеспечиваться за счет посылки уведомлений сразу же после возникновения события (аналогично подходу в протоколе OSPF [30]).

6. Реализация фаз этапа обмена информацией

Обмен данными между IDPS (фаза 11, остальные фазы в данном этапе используются для обоснованного выбора пути следования данных) можно вести аналогично протоколу OSPF [30, 31]. Такой подход обеспечивает следующие возможности:

−ограничение распространения информации за счет использования многоадресных рассылок;

−построение системы IDPS и доставка данных согласно иерархическому принципу;

−посылка уведомлений сразу же после возникновения события (для обеспечения быстрой сходимости сети и точной оценки рисков ИБ);

−организация многоканальной системы управления множеством IDPS за счет применения многопутевой рассылки (ограничивает представление злоумышленника относительно действий системы защиты);

−быстрое распространение ключевой информации (за счет присвоения высшего приоритета трафику криптографических ключей).

Выбор пути следования информации должен осуществляться на основе определенной метрики. Метрика (например, аналогично [32]) должна отображать также состояние телекоммуникационной сети и учитывать риск передачи информации по определенному пути.

Для протокола возможно использование модификации метрики протокола EIGRP [33]. Базовый вид метрики следующий:

$$M_{EIGRP} = \left[\left(K_1 \cdot B + \frac{K_2 \cdot B}{256 - L} + K_3 \cdot D \right) \cdot \frac{K_5}{K_4 + R} \right] \cdot 256, \qquad (1)$$

где $(K_1 \text{-} K_5)$ – переменные, которые определяются администратором сети для изменения приоритетов вычисления оценок (по умолчанию равны 1);

D – общая задержка передачи данных (с точностью до микросекунды);

B – минимальная пропускная способность (в кбит/с);

R – надежность (оценка от 1 до 255; 255 – наиболее надежно);

L – загрузка (оценка от 1 до 255; 255 – наиболее загружено).

EIGRP вычисляет пропускную способность и задержку как: $B = 10^7 / \text{пропускная способность интерфейса}$, $D = \text{задержка обработки данных}$. Чем лучше показатели интерфейса, тем меньше метрика.

Новая метрика должна учитывать два фактора: стойкость криптографической системы защиты информации и способность злоумышленника воздействовать на определенный сетевой канал или интерфейс.

Первый фактор $P_{\phi 1}$ требует определения вероятности как показателю, обратному времени (с точностью до микросекунды, как это определено в метрике EIGRP)), необходимому злоумышленнику для подбора ключа, которое зависит от степени развития компьютеров, способных проводить параллельные вычисления. Как можно увидеть из табл. 1, справедливо положение уточненного закона Мура

[34], что мощность передовых компьютеров увеличивается в два раза каждый год. Чем дольше используется криптографический ключ, тем более вероятна компрометация системы защиты.

Таблица 1. Суммарная вычислительная мощность суперкомпьютеров (по материалам сайта top500.org)

Год	Мощность, GFlops	Год	Мощность, GFlops
1993	2402	2003	924554
1994	4196	2004	1879877
1995	6909	2005	2632133
1996	11230	2006	5213548
1997	24278	2007	10579153
1998	44260	2008	25986996
1999	77240	2009	41004288
2000	131930	2010	64746740
2001	198187	2011	85179949
2002	456268		

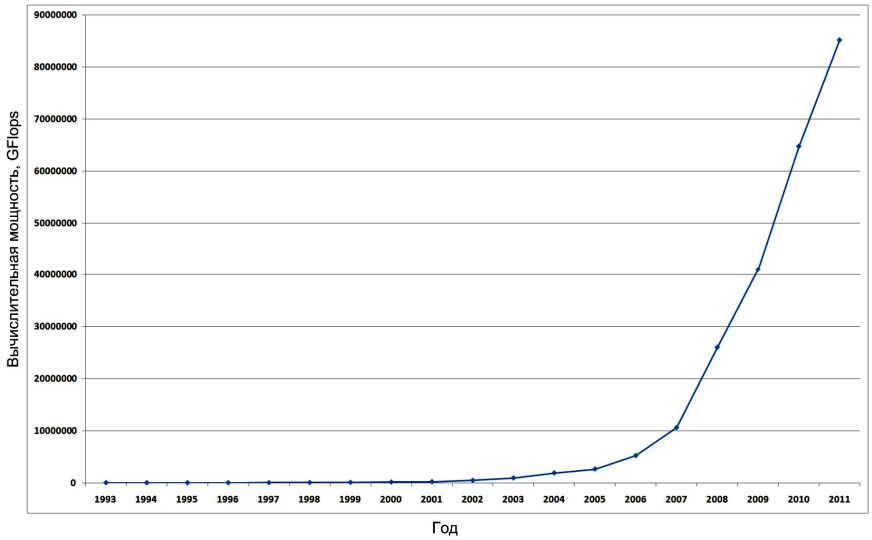

Рис. 2. Изменение суммарной вычислительной мощности суперкомпьютеров с течением времени

Поэтому вероятность компрометации системы за счет проведения экстенсивного криптоанализа $P_{\phi 1}$ в наиболее упрощенном виде можно определить как

$$P_{\phi 1} = 1 - \frac{1}{2^{t/T}}, \qquad (2)$$

где t – время использования системы (в микросекундах, для соответствия размерности времени задержки D);

T – константа, показывающая количество микросекунд в годе и равняется 31536000000000.

Предпочитаемым действием при приближении срока использования ключа является его смена, так как переход на увеличенную разрядность ключа может снизить стойкость системы к атакам, как в случае использования AES [35].

Таблица 2. Выбор показателя степени критичности

Номер, n	Описание типа уязвимости	Вероятность компрометации
1	Без выявленных уязвимостей	0.1
2	С уязвимостями, реализация которых требующими высоких ресурсных затрат	0.772
3	С уязвимостями, реализация которых требующими высоких интеллектуально-технологических затрат	0.988
4	С критическими уязвимостями, требующими определенной конфигурации системы	0.9964
5	С критическими уязвимостями, описание которых не опубликовано	0.9997
6	С критическими уязвимостями, описание которых опубликовано	0.99998

Второй фактор – вероятность компрометации канала (подсети) следования данных – $P_{ф2}$ определяется информацией об используемых аппаратной и программной платформах. Возможен следующий подход к определению показателя: градация уязвимостей по критичности с резким (например, степенным, табл. 2) увеличением уровня уязвимости и последующий выбор минимального уровня защищенности, свойственного самому ненадежному (в смысле ИБ) элементу ТКС. Даже системы без выявленных уязвимостей не могут считаться полностью защищенными, поскольку при определенных обстоятельствах уязвимости могут быть выявлены злоумышленником.

Поэтому вероятность компрометации системы, обусловленную уязвимостями используемых технологий $P_{ф2}$,в наиболее упрощенном виде можно определить как

$$P_{ф2} = 1 - \frac{1}{K_6 \cdot n^n}, \tag{3}$$

где K_6 – коэффициент, учитывающий возможность компрометации потенциально защищенной на сегодняшний день системы (может быть рекомендовано использование $K_6 = 1.11$, что соответствует вероятности компрометации 0.1);

n – номер показателя степени критичности ($n = 1..6$ – табл. 2).

Поскольку первый и второй фактор, в принципе, могут считаться независимыми, вероятности компрометации системы злоумышленником, анализирующим и первый и второй фактор, должны перемножаться:

$$M_{вероятн} = M_{EIGRP} \cdot K_7 \cdot P_{ф1} \cdot P_{ф2}. \tag{4}$$

K_7 – коэффициент, определяющий вычислительную мощность суперкомпьютеров на момент выбора алгоритма и ключа.

7. Выводы

На сегодняшний день не существует официальных стандартов управления системами IDPS и передачи информации между системами IDPS. Кандидатом на

данную роль является IDXP, однако он имеет ряд рассмотренных ограничений. Именно поэтому возникает задача разработки протокола (стека протоколов), решающего вопросы: проведения обнаружения различных видов IDPS в сети, обмена сигнатурами атак между IDPS, согласования действий по управлению состоянием сети и эффективного обмена информацией в потенциально незащищенной сети с нерегулярной структурой. Протокол должен учитывать различия в схемах работы IDPS и способах фиксации информации о событиях в сети, возможностях проведения анализа состояния сети, а также функциональных способностях устройств, выступающих в роли аккумулирующих данные элементов.

При вычислении маршрута следования данных между IDPS в сети необходимо использовать модифицированную метрику, которая учитывает вероятность компрометации пути следования информации и самой информации, если она передается в зашифрованном виде. Предлагаемая в работе модифицированная метрика соответствует правилу метрики EIGRP:

−при увеличении вычислительной мощности суперкомпьютеров метрика увеличивается, т.е. уменьшается потенциальная защищенность пути следования информации;

−при увеличении вероятности компрометации пути следования за счет криптоанализа, значение метрики увеличивается, т.е. будет выбираться путь, вероятность компрометации которого минимальна;

−при увеличении вероятности компрометации пути следования за счет уязвимостей ТКС, значение метрики увеличивается, т.е. будет выбираться путь, где количество потенциальных уязвимостей минимально.

Следует заметить, что в данной работе предлагается лишь прототип протокола и исследуются основные положения, которым необходимо удовлетворять при разработке реального протокола. Поэтому дальнейшие работы в данном направлении должны раскрывать и обобщать положения прототипа протокола.

Список литературы: 1. *Schneir B.* Schneier on security [Текст] – Wiley, 2008 – 336 p. 2. *Поповский В.В.* Защита информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2006. 3. RFC 3552 Rescorla E. Guidelines for writing RFC text on security considerations. IETF Network working group, 2003 – 44 p. 4. Stallings W. Data and computer communications. 9 Edition [Текст] – Pearson College Div, 2010 – 853 p. 5. NIST 800-94 Guide to intrusion detection and prevention systems (IDPS). National institute of standards and technology, 2007 – 127 p. 6. RFC 4767 Feinstein B. The intrusion detection exchange protocol (IDXP). IETF Network working group, 2007 – 28 p. 7. RFC 4765 Debar H. The intrusion detection message exchange format (IDMEF). IETF Network working group. 2007 – 157 p. 8. RFC 4852 Bound J. IPv6 Enterprise Network Analysis - IP Layer 3 Focus. IETF Network working group, 2007. – 32 p. 9. RFC 4861 Narten T. Neighbor Discovery for IP version 6 (IPv6). IETF Network working group, 2007 – 97 p. 10. RFC 4862 Thomson S. IPv6 Stateless Address Autoconfiguration. IETF Network working group, 2007 – 30 p. 11. RFC 3748 Aboba B. Extensible authentication protocol (EAP). IETF Network working group, 2004 – 67 p. 12. RFC 6071 Frankel S. IP security (IPsec) and Internet key exchange (IKE) document roadmap, IETF. Network working group. 2011 – 63 p. 13. *Поповский В.В.* Основы криптографической защиты информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2010. 14. RFC 3080 Rose M. The blocks extensible exchange protocol core. IETF Network working group, 2001 – 58 p.

15. RFC 3081 Rose M. Mapping the BEEP core onto TCP IETF Network working group, 2001 – 8 p. 16. ISO (International Organization for Standardization). ISO 8879:1986(E). Information processing — Text and Office Systems — Standard Generalized Markup Language (SGML). First edition — 1986-10-15. [Geneva]: International Organization for Standardization, 1986. – 155 p. 17. RFC 2045 Freed N. Multipurpose internet mail extensions (MIME) part one: format of internet message bodies, IETF Network working group, 1996 – 31 p. 18. RFC 5751 Ramsdell B. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. IETF, 2010, 45 p. 19. Kaeo M. Methodology for benchmarking IPsec devices. IETF Benchmarking working group. 2009 – 42 p. 20. RFC 2616 Fielding R. Hypertext Transfer Protocol - HTTP/1.1. IETF Network working group. 1999 – 176 p. 21. Ахо А Компиляторы: принципы, технологии и инструментарий, 2 издание. [Текст] – М.: Вильямс, 2008 – 1184 с. 22. RFC 3272 Awduche D. Overview and principles of Internet traffic engineering. IETF Network working group, 2002 – 71 p. 23. *Еременко А.С., Персиков А.В.* Проектирование итерационных многоканальных систем управления в сетях на основе обмена HTTP/XML-сообщениями // Праці УНДІРТ. – №4, Одесса. – 2004. – с.12-16. 24. Huang Q et all. Fast authenticated key establishment protocols for self-organizing sensor networks. [Текст] – Mitsubishi electric research laboratories, 2004 – 14 p. 25. Wireless LAN IEEE 802.15.4 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) IEEE computer society LAN MAN Standards Committee., – 323 p. 26. RFC 1035 Mockapetris P. Domain names – implementation and specification. Network working group, 1987 – 55 p. 27. RFC 4035 Arends R. Protocol modifications for the DNS Security Extensions. Network working group, 2005 – 53 p. 28. X.500 (ISO/IEC 9594-1) The Directory: Overview of concepts, models and services. 2005 – 34 p. 29. RFC 3418 Presuhn R. Management Information Base (MIB) for the Simple Network Management Protocol (SNMP). IETF Network working group, 2002 – 26 p. 30. RFC 2328 Moy J. OSPF version 2. IETF network working group. 1998 – 244 p. 31. RFC 5340 Coltun R. OSPF for IPv6. IETF network working group. 2008 – 94 p. 32. D. De Couto, D. Aguayo, J. Bicket, R. Morris, A High Throughput Path Metric for Multi-Hop Wireless Routing ACM Mobicom Conference, 2003– 13 p. 33. *Albrightson B., Garcia-Luna-Aceves J.J, Boyle J.* EIGRP – A fast routing protocol based on distance vector Proc. Interop 94, 1994 – 13 p. 34. Moore G. No exponential is forever [Электронный ресурс] / Intel corporation. – Режим доступа: http://download.intel.com/research/silicon/Gordon_Moore_ISSCC_021003.pdf – 15.09.2011 г. 35. Advanced Encryption Standard (AES). Federal Information Processing Standard Publication №197, 2001 – 51 p.

Поступила в редколлегию 13.09.2011

УДК 005.7: 005.8

В.И. ЧИМШИР**,** канд. техн. наук, доц., зав. каф., Измаильский факультет Одесской национальной морской академии, Измаил

СЛОЖНОСТЬ КАК ГРАНИЦА УПРАВЛЯЕМОСТИ СЛОЖНОЙ СОЦИОТЕХНИЧЕСКОЙ СИСТЕМОЙ

Выдвинута гипотеза существования зависимости информации о границах управляемости социотехнической системы от эффективности ее управления. Определены уровни описания социотехнической системы и причины повышения ее сложности. Описана модель социотехнической системы с точки зрения совокупности структур реализующих цели, технологий, факторов влияющих на функционирование.
Ключевые слова: социотехническая система, сложность, управляемость, проект, системный эффект, процесс, организационная структура.

Висунуто гіпотезу існування залежності інформації про межі керованості соціотехнічної системи від ефективності її управління. Визначено рівні опису соціотехнічної системи та причини підвищення її складності. Описана модель соціотехнічної системи з точки зору